EINDHOVEN UNIVERSITY OF TECHNOLOGY

Communication Theory (5ETB0)
Module 3.1

Alex Alvarado
a.alvarado@tue.nl

Information and Communication Theory Lab
Signal Processing Systems Group
Department of Electrical Engineering
Eindhoven University of Technology, The Netherlands

www.tue.nl/ictlab/

Module 3.1

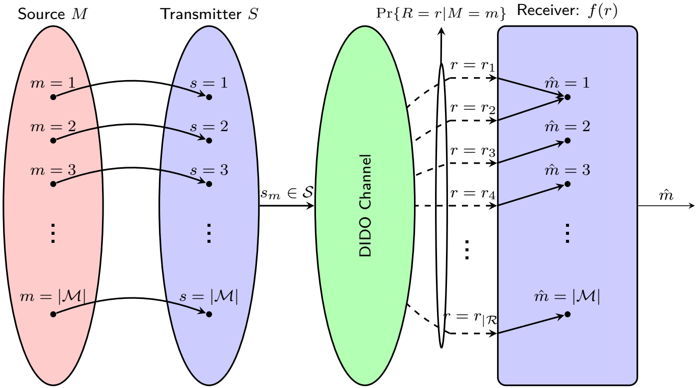
Presentation Outline

Definitions (1/2)

Definitions

- Source: Produces a *message* $m \in \mathcal{M} \triangleq \{1, 2, \ldots, |\mathcal{M}|\}$ with probability $\Pr\{M = m\}$ for $m \in \mathcal{M}$. The r.v. is M
- Transmitter: Sends a *signal* $s_m \in \mathcal{S}$ if message m is to be transmitted. The r.v. is S
- Channel: Produces output $r \in \mathcal{R}$ (r.v. is R) with conditional probability $\Pr\{R = r | S = s\}$
- Receiver: Forms an *estimate* $\hat{m}$ by observing the received channel output $r \in \mathcal{R}$ using a mapping $\hat{m} = f(r) \in \mathcal{M}$. The r.v. is $\hat{M}$

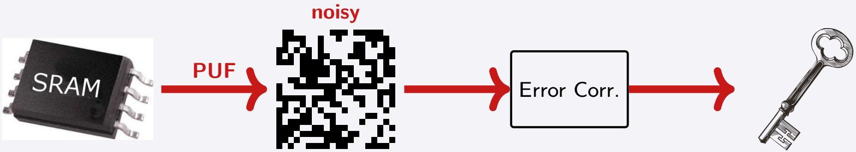
Definitions (2/2)



Motivation for DIDO Channels: SRAM-PUF

Average Error Probability

- Use power-on value of SRAM to generate cryptographic keys
- Error-Correcting Codes required to reliably reconstruct the key from noisy binary values
- RESCURE project: improve security, reliability, performance



Rescure

eurostars™

Co-funded by EUREKA member countries and the European Union Horizon 2020 Framework Programme

Module 3.1

Presentation Outline

Error Probability Definitions

The Detection Problem

- For a given channel, find the best **decision rule** $f(r)$
- Best in what sense? Error probability...

Average Error Probability

The **probability of error** is defined as

$$P_{\mathrm{e}} \triangleq \Pr\{\hat{M} \neq M\}. \tag{1}$$

The **probability of correct decision** is defined as

$$P_{\mathrm{c}} \triangleq \Pr\{\hat{M} = M\} = 1 - P_{\mathrm{e}}. \tag{2}$$

Optimum Receiver

A receiver is optimum if it minimizes the error probability P_{e}.

Correct Probability via Joint PMF (1/2)

Average Error Probability

The correct probability can be expressed as

$$
\begin{aligned}
P_{\mathsf{c}} &= \Pr\{M = \hat{M}\} \\
&= \Pr\{M = f(R)\} \\
&= \sum_{r\in\mathcal{R}} \Pr\{R = r, M = f(r)\} \\
&= \sum_{r\in\mathcal{R}} \sum_{m\in\mathcal{M}} \Pr\{R = r, m = f(r)|M = m\} \Pr\{M = m\} \\
&= \sum_{m\in\mathcal{M}} \sum_{r\in\mathcal{R}} \Pr\{R = r, m = f(r)|M = m\} \Pr\{M = m\} \\
&= \sum_{m\in\mathcal{M}} \sum_{r\in\mathcal{R}: f(r)=m} \Pr\{R = r|M = m\} \Pr\{M = m\} \\
&= \sum_{m\in\mathcal{M}} \sum_{r\in\mathcal{R}: f(r)=m} \Pr\{M = m, R = r\}
\end{aligned}
$$

Correct Probability via Joint PMF (2/2)

Error Probability Computation: A Recipe

- We showed that:

$$P_{\mathsf{c}} = \sum_{m\in\mathcal{M}} \sum_{r\in\mathcal{R}:f(r)=m} \Pr\{M=m, R=r\}$$

- Make a table with $\Pr\{M=m, R=r\}$ for all possible combinations of m and r
- For each $M=m$, find all columns where $f(r)=m$, and sum them up
- Alternatively, for each $R=r$, identify the entry in the table that the detection rule $f(r)$ will choose

Example 3.1 (1/4)

Applying the Recipe

- Tx signals: $s \in \mathcal{S} = \{s_1, s_2\}$ ($|\mathcal{M}| = 2$). Rx signals: $r \in \mathcal{R} = \{a, b, c\}$
- A-priori probabilities:

m	$\Pr\{M = m\}$
1	0.4
2	0.6

- Conditional probabilities:

m	$\Pr\{R = a \| S = s_m\}$	$\Pr\{R = b \| S = s_m\}$	$\Pr\{R = c \| S = s_m\}$
1	0.5	0.4	0.1
2	0.1	0.3	0.6

- Decision rule: $f(r) = 1$ if $r \in \{a, b\}$ and $f(r) = 2$ if $r = c$
- Joint probabilities:

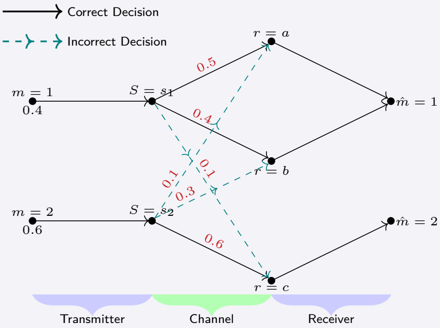
m	$\Pr\{M = m, R = a\}$	$\Pr\{M = m, R = b\}$	$\Pr\{M = m, R = c\}$
1	0.20	0.16	0.04
2	0.06	0.18	0.36

- Correct probability is $P_\mathsf{c} = 0.2 + 0.16 + 0.36 = 0.72 \Rightarrow P_\mathsf{e} = 0.28$

Example 3.1 (2/4): A different view

A Graphical Interpretation

$$P_{\mathrm{e}} = \Pr\{\hat{M} \neq M\} = \sum_{m \in \mathcal{M}} \Pr\{\hat{M} \neq M | M = m\} \Pr\{M = m\} \quad (3)$$



Error probability is $P_{\mathrm{e}} = 0.4 \cdot 0.1 + 0.6 \cdot (0.1 + 0.3) = 0.28 \Rightarrow P_{\mathrm{c}} = 0.72$

Module 3.1

Presentation Outline

Example 3.1 (3/4)

Maximum Likelihood Detection

- Can we increase P_{c} by improving $f(r)$?

$$P_{\mathsf{c}} = \sum_{m \in \mathcal{M}} \sum_{r \in \mathcal{R}: f(r)=m} \Pr\{M=m, R=r\}$$

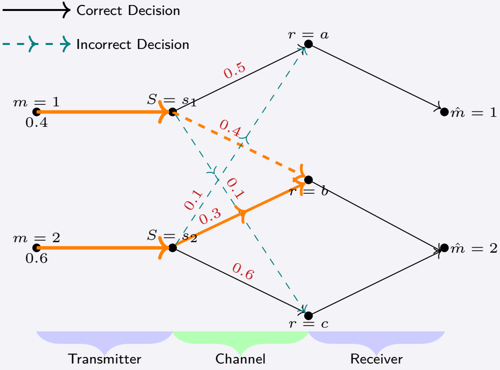
- For each column, the decision rule picks one row
- The example:

m	$\Pr\{M=m, R=a\}$	$\Pr\{M=m, R=b\}$	$\Pr\{M=m, R=c\}$
1	0.20	0.16	0.04
2	0.06	0.18	0.36

- A higher correct probability is $P_{\mathsf{c}} = 0.2 + 0.18 + 0.36 = 0.74 \Rightarrow P_{\mathsf{e}} = 0.26$

Example 3.1 (4/4): A different view

A Graphical Interpretation



Error probability is $P_{\mathsf{e}} = 0.4 \cdot (0.1 + 0.4) + 0.6 \cdot 0.1 = 0.26 \Rightarrow P_{\mathsf{c}} = 0.74$

Summary Module 3.1

Take Home Messages

- DIDO Channels and problem definition
- Error probability definition and calculations
- Detection can be improved

Communication Theory (5ETB0)
Module 3.1

Alex Alvarado
a.alvarado@tue.nl

Information and Communication Theory Lab
Signal Processing Systems Group
Department of Electrical Engineering
Eindhoven University of Technology, The Netherlands

www.tue.nl/ictlab/